Introduction
to SCS Computing

SCS Computing Facilities
School of Computer Science
Carnegie Mellon University

SCS Help Desk
Gates Hillman Complex 4203
Monday—Friday 9am to 5pm
(412) 268-4231
help@cs.cmu.edu

SCS Help Pages
http://www.cs.cmu.edu/~help
## 3. Electronic Mail

3.1. Delivery Options 15
3.1.1. Delivery to IMAP 15
3.1.3. Delivery Off-Site 15

3.2. IMAP 15
3.2.1. Supported Standalone IMAP Clients 16
3.2.2. IMAP Webmail Clients 16
3.2.3. Using the SCS Out of Office Tool 17
3.2.4. Filtering Mail With IMAP 19
3.2.5. Message Auto-Expiration with IMAP 19

3.3. Email Security 21
3.4.1. Attachments and Trojans 21
3.4.2. Phishing 22
3.4.3. Displaying Remote Images 22

3.4. Spam and Virus Detection and Filtering 23
3.5.1. Server-Side Tagging and Filtering 23
3.5.2. Client-Side Spam Filtering 23

3.5. Email Account Preferences 23
3.6.1. The Email Attribute Tool 23
3.6.2. Your Preferred Email Address 24
3.6.3. Your Email Local Addresses 25
3.6.4. Your Email Forwarding Address 27
3.6.5. Blocking Spam With Grey Listing 28
3.6.6. Discarding Spam 28

3.6. Mailing Lists 30
3.7.1. Creating a Mailing List 30
3.7.2. Mailing List Administration 30
3.7.3. Mailing List Etiquette 30

## 4. Printing 33

4.1. Printing Etiquette 33
4.2. Getting Help 33
4.3. Lists of Printers 33

## 5. Networking 35

5.1. SCS Network Use Policies 35
5.1.1. Connecting Hosts to the Network 36
1. Welcome

Welcome to the School of Computer Science at Carnegie Mellon University!

This document offers an overview of the SCS computing environment for new users at the School of Computer Science. This is not intended to be a comprehensive set of instructions, but a good place to start gaining familiarity with the computing environment.

This document is available in a PDF version:


Throughout this guide we will provide links to more information on our Help Pages:

http://www.cs.cmu.edu/~help/

1.1. Getting to Know SCS Computing Facilities

1.1.1. What We Do

The SCS Computing Facilities staff supports all aspects of computing for the School of Computer Science. We provide:

**End User Support**
- SCS Help Desk
- User Consulting
- Research
- Documentation
- Technical Procurement
- Account Management
- Operations
- Loaner Equipment
- Resource Management

**Computing Support**
- Hardware Maintenance, Upgrades & Repair
- Software Installation, Maintenance & Upgrades
- Requirements Consulting
- Product Research
- Software Licensing
- Virtual Machines

**Infrastructure Support**
- Authentication
- Email Services
- Calendaring Services
- Printing Services
- Archive Backup Services
- Data Protection Service
- Web Services
- Network Infrastructure
- Security Monitoring
- High Performance Computing

...and anything else related to the SCS computing environment. If you have questions, please ask us!

1.1.2. What We Can Help With

While we are unable to assist directly with problems, requests, or concerns relating to other computing environments on campus (Andrew, ECE, etc.), we are happy to act as liaisons to help address any issues you may have that involve computing outside of SCS.
1.1.3. The Help Desk
The SCS Help Desk is the place to go for support; you are welcome to send us an email, give us a call, or drop by in person with any and all of your questions and requests.

Help Desk Hours
The Help Desk is open:

9am to 5pm
Monday—Friday

Visiting the Help Desk in Person
The Help Desk is located at:

Gates Hillman Complex
Room 4203

Reaching the Help Desk by Phone
On campus:

x8-4231

Off campus:

(412) 268-4231

Reaching the Help Desk via Email
The Help Desk accepts email at:

help@cs.cmu.edu

After Hours Support
After hours support is provided by SCS Operations. The operations desk can be reached by phone at:

(412) 268-2608
1.1.4. **The Help Pages**

The SCS Help Pages are our online resource for documentation, tools, and news about computing at SCS. You can use the Help Pages to learn more about the computing environment, manage your passwords and account preferences, and keep up to date with current events that affect the facility.

The help pages can be found at the following URL:

http://www.cs.cmu.edu/~help

1.1.5. **Useful Links for User Support**

- Change Your Kerberos and Windows Passwords
  https://webiso.cs.cmu.edu/instance/

- Check Your Email With the Webmail Client
  http://webmail.cs.cmu.edu/

- Change Your Email Preferences
  https://www.fac.cs.cmu.edu/corvid/lookup/

- Set an Out Of Office Message
  https://webapps.cs.cmu.edu/OutOfOffice/

- Find a Phone Number
  http://www.cs.cmu.edu/directory/
  http://directory.andrew.cmu.edu/

- Publish a Web Page
  http://www.cs.cmu.edu/~help/web_publishing/web_publishing_intro.html

1.1.6. **Useful Links for Computing Support**

- Register Computer Equipment for the SCS Wired Network
  http://www.cs.cmu.edu/~help/networking/netregister.html

- Recommended Hardware Configurations
  http://www.cs.cmu.edu/~help/purchasing/recommended_pcs.html
1.2. Getting to Know the School of Computer Science

The SCS community has developed a set of rules and customs for behavior that is generally considered acceptable by others in the Department. These rules suggest ways to conserve and share public resources, as well as how to best be a reasonable and responsible member of the SCS community. We present some guidelines to help you get off to a good start.

1.2.1. Shared Computing Resources

Help keep our computing environment safe and working well:

- Keep your account and its password private. You are responsible for anything done from your account.
- Notify SCS Computing Facilities in advance and read the section on Network Usage Policy before connecting any computer or other networked device to our network.
- If you need to make multiple copies of a document, use a photocopier.
- Print large documents at off-peak hours.
- Respect others’ privacy.
- Do not read someone else’s files unless you know you have permission: if in doubt, always ask for permission, even if that person has not employed any file protection mechanisms.
- Consider printer output private.
- Make sure that all of your computers have been kept up to date with all of the current patches.

There are socially-acceptable ways of using digital communications:

- Keep messages short.
- Don’t send anonymous messages or hate mail—these actions can result in the loss of your account privileges.
- Do not use government-sponsored equipment and resources or post messages outside of SCS for commercial gain.
1.2.2. Locating People

There are several online directories that can easily be used to get information about members of the University community.

**SCS Directory**

The School of Computer Science maintains an online directory of all current faculty, staff, and graduate students who are part of the SCS community. The directory can be accessed at the following website:

[http://www.cs.cmu.edu/directory/](http://www.cs.cmu.edu/directory/)

**Campus Directory**

Carnegie Mellon maintains an online directory of all current faculty, staff, and students affiliated with the university community. The directory can be accessed at the following website:

[http://directory.andrew.cmu.edu/](http://directory.andrew.cmu.edu/)
2. The SCS Environment

2.1. End-User Resources

Most departments in the School of Computer Science will provide incoming faculty, students and staff with a desktop or a laptop computer that has been configured by SCS Computing Facilities.

For more about support for end-user resources, please see End-User Computing on page 5151.

2.2. Personal Resources

You are welcome to use personally owned computers, mobile devices, and other equipment within the SCS environment.

Personal equipment that causes problems on the SCS network may be blocked from network access as a result; please see §1.1. SCS Network Use Policies on page 34.

For more about connecting personally owned computers, mobile devices, and other equipment to the wireless network, please see §5.5.1. Computing Services Wireless in SCS on page 40.

Support for personally owned equipment is limited; we can only provide best-effort support, and support for personally owned equipment is not given priority. Personally owned equipment is ineligible to enroll in hardware, software, or backup support from SCS Computing Facilities staff.

2.3. Shared Resources

SCS Computing Facilities provides remote access to both Windows and Linux services. Windows services are provided by the Windows Terminal Services system, and Linux services are provided by a set of general purpose Linux systems.

Accessing Windows Terminal Services

You may access Windows services from a Linux host through Windows Terminal Services. You may access Windows applications, such as Microsoft Word, Excel, or PowerPoint from a Linux host using Windows Terminal Services. This is described on the SCS Computing Facilities help pages:

http://www.cs.cmu.edu/~help/unix_linux/terminal.services.html

You may request access to Windows Terminal Services through the SCS Help Desk.
Accessing The General Purpose Linux Services

The Linux General Purpose (GP) services may be accessed via any SSH client. Use an SSH client to connect to the following hostname:

linux.gp.cs.cmu.edu

You can log in with your SCS username and Kerberos password.

The Linux GP Services can be used for access to command-line or X-Windows based applications, but there are several limitations:

- You will not have a home directory on the local disk — you should use your AFS home directory to store any files (see AFS on page 43).
- Programs that use large amounts of memory or CPU cycles are discouraged, as this is a shared resource.

For more information about using the Linux GP Services, please see the help pages:

http://www.cs.cmu.edu/~help/unix_linux/linux/linux_gp.html

2.4. Passwords

Here in the School of Computer Science, you will have several types of passwords. Below is an overview of these passwords and their purposes.

2.4.1. Kerberos Passwords

<table>
<thead>
<tr>
<th>Type of Password</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos</td>
<td>This is your main username/password combination in SCS. This password is used to log in to any website or service protected by SCS Web Authentication.</td>
</tr>
<tr>
<td></td>
<td>This password is also used to log in to Linux machines in the SCS Environment. This username and password are assigned to you when you first join the SCS community. You will need to change this password; please see Changing a Kerberos Instance Password on page 11.</td>
</tr>
<tr>
<td>/mail (Kerberos instance)</td>
<td>This password is used exclusively with your SCS email. You will need to create this instance and set a password before you will be able to log in to your mail account with a desktop mail client.</td>
</tr>
<tr>
<td></td>
<td>This password is not created for you initially.</td>
</tr>
<tr>
<td>/root (Kerberos instance)</td>
<td>This is a special Kerberos instance for people who need to do advanced system administration on Linux machines.</td>
</tr>
<tr>
<td></td>
<td>This password is not created for you initially.</td>
</tr>
<tr>
<td>/remote (Kerberos instance)</td>
<td>Use this password to authenticate to the remote services VPN and iPass.</td>
</tr>
<tr>
<td></td>
<td>This password is not created for you initially.</td>
</tr>
</tbody>
</table>
2.4.2. Windows Domain Password

<table>
<thead>
<tr>
<th>Type of Password</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Domain</td>
<td>This password is used to authenticate to Windows-based machines and services, such as:</td>
</tr>
<tr>
<td></td>
<td>• Logging in to Windows machines</td>
</tr>
<tr>
<td></td>
<td>• Printing from Windows and Mac computers to SCS printers</td>
</tr>
<tr>
<td></td>
<td>• Mapping windows network drives between machines in the SCS Domain</td>
</tr>
</tbody>
</table>

2.5. Password Security

It is important when setting your passwords to choose a strong password. A common or weak password is a means by which any account can be broken into by an attacker. A strong password is one that is at least eight characters, and includes a combination of letters, numbers, and symbols. Your password should be easy for you to remember, but difficult for others to guess.

It should not be a word that is found in the dictionary.

The easiest way to create a strong password that you won't have to write down is to come up with a pass phrase. A pass phrase is a sentence that you can remember, like:

My son Aiden is three years older than my daughter Anna.

You can make a strong password by using the first letter of each word of the sentence, for example, msaityotmda. However, you can make this password even stronger by using a combination of upper and lowercase letters, numbers, and special characters that look like letters. For example, using the same memorable sentence and a few tricks, your password is now M$8ni3y0tmd@.

Note: Never use a password that has been published as an example for your actual account password

2.6. Changing Passwords

It is a good idea to change your passwords on a regular basis.

We recommend changing your passwords every six months. One way to remember to do this is to change your passwords seasonally; for example, you may choose to change your passwords at the beginning of Spring and Autumn. It might also be easy to remember to change your passwords at the start of every semester.

If you need any assistance with any password change, please visit the SCS Help Desk in person. Please remember to bring valid Photo ID for any password changes.
2.6.1. Managing Kerberos Instances

To create, remove, or update your Kerberos instances, please go to the SCS Kerberos Instance Manager in any web browser:

https://webiso.cs.cmu.edu/instance

To use the SCS Kerberos Instance Manager, you will need to authenticate via WebISO (see Figure 1):

Once authenticated, you can use the SCS Kerberos Instance Manager to create new instances and change instance passwords (see Figure 2):

Creating a Kerberos Instance

You can use the SCS Kerberos Instance Manager to create a new instance. You may need to create an instance to read mail, or to use remote services; please see §2.4.1. Kerberos Passwords on page 8 for more information about common instances.

To create a new instance with the Instance Manager:
1. Click **Create** next to the instance you wish to create.
2. Enter and verify the password for the new instance.
3. Click **Create Instance** to create the instance and set the password.

**Changing a Kerberos Instance Password**

If a Kerberos instance already exists, but you need to change the password for that instance, you can use the SCS Kerberos Instance manager to reset that password.

To change the password of an existing instance with the Instance Manager:

1. Click **Change Password** next to the appropriate instance.
2. Enter and verify the new password.
3. Click **Change Password** to set the new password.

**2.6.2. Windows Domain Passwords**

A common or weak password is a means by which Windows hosts can be broken into by an attacker. In particular, SCS Windows domain accounts are often the target of break-ins. You should make sure that your Windows domain password is a strong password.

In addition, if you are installing a networked service such as MS SQL server, you should make sure that any passwords for that service are reset to a strong password that is something other than the default (this is especially true of the *sa* account on SQL server). Please ensure that all necessary patches have been installed.

**2.6.3. Changing Your Windows Domain Password**

You can use the SCS Kerberos Instance manager to change your windows domain password.

To change your windows domain password with the Instance Manager:

1. Click **Change Password** next to the entry for your Windows account.
2. Enter and verify the new password.
3. Click **Change Password** to set the new password.

**2.6.4. Forgotten Passwords**

If you have forgotten any of your passwords and need assistance in resetting them, please visit the SCS Help Desk in person. Please remember to bring valid Photo ID for any password changes.
2.7. Logging In

2.7.1. SCS Authentication
There are many different username / password combinations that are used in the SCS computing environment, but the three most common are Kerberos, Mail, and Windows.

When your SCS account is created you will receive the following:

- A Kerberos username and password; these have been sent to you via email.
- A Windows domain password.

Note: While you will use the same username everywhere in the SCS environment, these passwords must not be the same.

2.7.2. Logging on to Windows
On a Windows-based machine, you will be prompted to click any button to log in.

Once you click a button, you will see a login window with two fields: Username and Password. Below the password field it should read Log on to: SCS (see Figure 3).

You may have received an email with your username and initial Windows password when your account was created. Use these credentials to log into your Windows computer for the first time.

If you have not received this email, or if your initial password does not work, please contact the SCS Help Desk.

2.7.3. Logging on to Linux
In order to log in to an SCS Linux machine you need both an SCS Kerberos account and a local account on the particular machine to which you wish to log in to. Contact the SCS Help Desk and ask them to create this local account once your main SCS user account has been created and you have a specific Linux machine you wish to access (if you have received a graduate student machine from your department you will have an account on the machine assigned to you). Once this local account has been created, simply use your Kerberos username and password to log in to the machine (see Figure 4).
2.7.4. Logging on to Mac OS X

To log in to a SCS Mac computer running OS X you will need a local user account. Local user accounts on Mac computers are added when the machine is initially configured by SCS Computing Facilities. If you have a Mac computer, your initial account password will be provided to you.

To log in to your SCS Mac computer, use your SCS username and local password (see Figure 5).

2.8. Reserving Rooms

In SCS we use a web service to manage rooms. All members of the SCS community with an active user account have privileges to view room reservations in public and semi-private spaces.

This service is named Meeting Room Manager (MRM). MRM is available at the following url:

https://www.netsimplicity.net/SCS/

Your MRM account will be automatically created the first time you use the service.

More information about MRM is available on the help pages:

http://www.cs.cmu.edu/~help/resource_management/
3. Electronic Mail

You may choose to have any email sent to your SCS email account delivered to our local Exchange server, delivered to our local IMAP server, or forwarded to an account on an external mail service.

If your email is delivered locally, we support a wide range of email clients for local and remote access.

3.1. Delivery Options

Your incoming email will only be directed to one place for delivery:

- SCS IMAP Server
- Delivery to an address external to SCS

3.1.1. Delivery to IMAP

You may choose to have your email delivered locally to an account on our IMAP server.

You may use IMAP clients to access your email on the IMAP server. The IMAP server is very flexible; we support a wide range of IMAP clients for all of the supported operating systems in the facility. We are also happy to do what we can to help configure other IMAP clients to work with our IMAP server.

3.1.2. Delivery Off-Site

You may choose to have your email sent off-site.

**Note:** By policy, we do not forward mail that is tagged as Spam off-site. If you forward mail to an outside account, some of your mail may not be delivered.

If you have a separate email account hosted outside of the department, you can have all of your email forwarded to that account.

While many of our users find this to be a convenient option, this is not a recommended configuration. If you opt to have your mail forwarded, there is little we can do to help support email accounts hosted by providers outside of the School of Computer Science.

3.2. IMAP

If you choose to use the SCS IMAP server for email storage, you will need to use an email client to read and send email. We support several popular mail clients on all of the supported operating systems here in SCS, as well as webmail. We can provide support for other IMAP clients and/or personal computing devices on a best effort basis.
3.2.1. Supported Standalone IMAP Clients
We support a wide range of IMAP clients:

**Windows**
- Thunderbird
- Outlook

**OS X**
- Thunderbird
- Mail.app
- Outlook

**Linux**
- Thunderbird
- Alpine

Configuration instructions for supported email clients can be found at the following URL:

http://www.cs.cmu.edu/~help/mail_news/index.html#clients

3.2.2. IMAP Webmail Clients
If your mail is being locally delivered to the SCS IMAP server, you have a choice of two available webmail clients with which to access your mail of the web.

To access either webmail client, visit the following URL in any modern web browser:

http://webmail.cs.cmu.edu/

...which will allow you a choice of which webmail client to use.

**Available Webmail Clients**
We support two webmail clients for our IMAP server:
- Roundcube
- SquirrelMail

Roundcube is a modern webmail client that offers much of the standard functionality of a stand-alone mail client. The interface uses current web technologies to enable features like drag & drop and multiple selections.

SquirrelMail is a mature webmail client that offers much of the standard functionality of a stand-alone mail client. The interface is simple, and works well in older browsers.

You may switch back and forth between IMAP webmail clients as much as you like; if you decide that one of them better suits your needs, you can bookmark it for easier access.
Authenticating to Webmail

To log in to either webmail client via SCS WebISO:

1. Enter your User ID.
2. Enter your mail instance password.
3. Select /mail as the instance.
4. Click Log In.

You are now logged into the SCS Webmail client of your choice.

For more information about the webmail client, please see the following web page at the SCS Help Pages:

http://www.cs.cmu.edu/~help/mail_news/webmail/

3.2.3. Using the SCS Out of Office Tool

If you have plans to be out of the office for an extended period, you may want to have an automatic email reply to let people know.

Where you set an Out of Office message depends on where you email is delivered. If your email is delivered to the SCS IMAP servers, you may use the SCS Out of Office Tool.

To access the SCS Out of Office Tool to create, change, or disable your away message, visit the following web page in a web browser:

https://webapps.cs.cmu.edu/OutOfOffice/

...which will redirect you to the SCS WebISO authentication server.

To authenticate to the Out of Office Tool using the SCS WebISO Authentication Service, perform the following steps:

1. Enter your User ID.
2. Enter your mail instance password.
3. Select /mail as the instance.
4. Click Log In.

Once you have authenticated to the Out of Office Tool, you will be able to view, adjust, and/or disable your away message.
Setting An Out Of Office Message

You may only have one away message set at a time. If you do not already have a current away message set, you can set up a new away message with the following steps:

1. Select the dates and times of your departure and return:

2. Compose a subject line for your away message (you may use the variables listed at the bottom of the page to customize the subject line of your away message):

3. Compose the body of your away message (you may use the variables listed at the bottom of the page to customize the body of your away message):

4. Click Save to activate your Out of Office message.

Changing An Out Of Office Message

If your plans change, and you need to alter your current Out of Office message, log in to the Out of Office tool as above. You will see your current away message. Make any necessary changes to your away message, then click Save to activate your new away message.
Disabling An Out Of Office Message

The Out of Office Tool will automatically disable your away message on your return date; you do not need to do anything to turn off your Out of Office Message if you return on the expected date.

If you return unexpectedly early and need to disable you away message, log in to the Out of Office tool as above. You will see your current away message. Click **Disable** to turn off your Out of Office message.

3.2.4. Filtering Mail With IMAP

Filtering Mail at the IMAP Server

Our IMAP server implements the Sieve scripting language which allows users to define operations such as filing of mail messages based on header comparisons (anti-spam filing, for example) and forwarding mail to alternative addresses.

Sieve scripts are simple text files that are uploaded to, and run on, the IMAP server. In our environment, there are two options for placing Sieve scripts onto our IMAP server:

- Through the WebSieve interface
- Via a command line interface run from an SCS Linux machine

Managing Server-Side IMAP Filters With Websieve

The WebSieve interface offers both a basic and advanced method of manipulating Sieve scripts on the server.

http://webmail.cs.cmu.edu/websieve/

The basic interface is useful for simple operations, such as enabling and disabling the default spam filter and maintaining simple whitelists and blacklists of allowed and blocked senders.

**Note:** Extensive use of whitelists and blacklists is not recommended.

WebSieve also offers an advanced interface that allows for direct manipulation and editing of scripts on the server.

For more information, please see:

http://www.cs.cmu.edu/~help/mail_news/intro.sieve.html

3.2.5. Message Auto-Expiration with IMAP

The IMAP server offers users the ability to configure individual mailboxes to remove messages automatically after a specified period. Messages in each mailbox with an expiration setting will be deleted when their age exceeds the expiration limit. The SCS Webmail system includes an interface for managing these settings.
Caveats
The read/unread status of a message makes no difference to automatic expiry; even unread messages will be deleted once they are older than the expiration date set on the mail folder. Do not set expirations on infrequently-checked mailboxes that are likely to contain unread messages for extended periods of time.

The server uses the `Date:` header to determine message age. Messages with a `Date:` header in the future will not be deleted until after the future date plus the expiration time passes. Conversely, messages with an incorrect `Date:` header in the past may be deleted sooner than expected. Since messages with wildly incorrect `Date:` headers tend to be spam, this mechanism should not cause a problem for most users.

The interface deliberately prevents you from setting an expiration period on your INBOX. If you have a specific need for that arrangement (for example, you regularly file all mail into sub-folders and your INBOX contains only unimportant or unwanted mail), please contact the SCS Help Desk. We will enable this setting at your request.

Using the Mailbox Expiration Tool
To use the mailbox expiration tool:

1. Navigate to the SquirrelMail webmail client at http://webmail.cs.cmu.edu/squirrelmail
2. Log in to SquirrelMail.
3. Click on the Options link near the top of the window.
4. Click on Message Expiration Options.
5. You should now see the Mailbox Expiration Tool:

<table>
<thead>
<tr>
<th>Mailbox Expiration</th>
<th>Set New Expiration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Expire after</td>
</tr>
<tr>
<td>INBOX.SPAM</td>
<td>30 days (max 180)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Current Expiration Settings</th>
<th>Expires after</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td></td>
</tr>
</tbody>
</table>

Setting an Expiration
To set an expiration on a folder:

1. Select the folder you wish to configure under Folder.
2. Select the expiry period under Expire after.
3. Click Set.
A status message will confirm that the expiration has been set on the mailbox.

**Viewing Active Expirations**

You may set an expiry on as many or as few folders as you wish. To help keep track of the current expiries for your account, the Mailbox Expiration tool lists these under **Current Expiration Settings**.

In this example, the folder **INBOX.SPAM** is set to remove mail that is more than 30 days old:

<table>
<thead>
<tr>
<th>Folder</th>
<th>Expires after</th>
</tr>
</thead>
<tbody>
<tr>
<td>INBOX.SPAM</td>
<td>30 days</td>
</tr>
</tbody>
</table>

To remove expiration from a mailbox, click **Remove**. A status message will confirm that the expiration setting has been removed.

### 3.3. Email Security

Computer viruses, Trojans, and other malware often try to infect your computer via email. Bad actors may also try to use email to lure you into providing sensitive information. It is important to exercise caution when dealing with email that appears suspicious, or is sent from an untrusted source.

SCS Computing Facilities staff will *never* ask you for your password.

If you have any questions or suspicions about a particular message, please contact the Help Desk.

#### 3.3.1. Attachments and Trojans

To reduce the likelihood of being infected by a virus or a Trojan via an email message, use the following common sense guidelines.

Do not run or open email attachments unless:

- you know the sender
- you expect an attachment from that person
- the subject line of the mail and type of attachment fit with what you’re expecting from the sender

Do not run programs from untrusted sources.
Spam mailers and email viruses have the ability to forge messages to make it appear as if the email is coming from someone you know. If you have suspicions about where an email message came from, please contact the SCS Help Desk.

### 3.3.2. Phishing
Phishing is a tactic of convincing someone to reveal sensitive information:

- passwords
- credit card numbers
- banking details

...or other similar information through misdirection, deception, or other subterfuge. Phishing often takes the form of mail messages.

Phishing messages often request or demand personal information, usually with some sense of urgency or threat that a service or opportunity is about to expire. If you receive a notice of loss of access or an impending fine that looks legitimate, treat the message with caution and verify the contents of the message through other means (via phone, etc.) before following the instructions in the message.

Phishing attempts via email often have clickable links embedded in the message, which can misrepresent themselves as links to the websites of well-known companies or services. If you are at all suspicious of a message containing clickable links, always manually check the link before clicking on it.

**Note:** SCS Computing Facilities staff will never ask you for your password.

If you encounter a message that demands personal details, always check to make very sure the message is legitimate. If you have any questions about a suspicious piece of email, or would like assistance with verification, please contact the SCS Help Desk.

### 3.3.3. Displaying Remote Images
Most modern mail clients have the ability to display images embedded in an email message. Sometimes, these embedded images are not included in the message itself, but are served off of a remote webserver.

These remote images can pose a privacy risk. If the sender is monitoring the webserver that is serving the images in your mail, when you read the message and load the remote images, the sender will be able to verify your email address and note when the email was read.

Most modern mail clients will allow you to turn off automatic loading of remote images. If the option is available, we recommend that you set your client to only load remote images on demand, and then only load remote images from trusted sources.
3.4. Spam and Virus Detection and Filtering

3.4.1. Server-Side Tagging and Filtering
All incoming email is scanned for spam content and viruses. We use the Pure Message filtering service offered by Sophos to score messages for spam and flag messages with malicious attachments.

Pure Message works by applying a set of rules and checks to each piece of email. If Pure Message discovers suspicious patterns in the email, the service will tag the piece of email as spam. By default, email that has been tagged as spam will be automatically filed into your SPAM folder; you may also set your preferences to discard spam entirely (see §3.5.6. Discarding Spam on page 28).

Note: By policy, email that has been tagged as spam will not be forwarded to an account outside of the School of Computer Science.

If Pure Message discovers a virus in an attachment, the message will be delivered with the attachment removed and [PMX-Virus] prepended to the Subject header.

3.4.2. Client-Side Spam Filtering
Many email clients also offer built-in SPAM filtering. Client-side SPAM filters usually work by training; you can teach the filter what to treat as SPAM, and the filter will adapt to your incoming mail as it learns to discern good mail from unwanted mail.

Because client-side SPAM filters can sometimes treat legitimate mail as SPAM, we recommend using client-side filters only when absolutely necessary.

3.5. Email Account Preferences

3.5.1. The Email Attribute Tool
The Email Attribute Tool allows you to view or change several preferences which determine how your email is handled when it arrives at the School of Computer Science. You can use the Email Attribute tool to specify:

- Your primary published email address
- Which email addresses are valid for your account
- Where your mail should be delivered
- How spam should be handled
Connecting to the Email Attribute Tool
To access the Email Attribute Tool to view or change your account preferences, visit the following web page in a web browser:

https://www.fac.cs.cmu.edu/corvid/lookup/

...which will redirect you to the SCS WebISO authentication server.

To log in to the Email Attribute Tool via SCS WebISO, you will need to perform the following steps:

1. Enter your User ID.
2. Enter your mail instance password.
3. Select None as the instance.
4. Click Log In.

<table>
<thead>
<tr>
<th>User ID: example</th>
<th>Instance</th>
<th>@CS.CMU.EDU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password: *******</td>
<td>None</td>
<td>/mail</td>
</tr>
</tbody>
</table>

Using the Email Attribute Tool
Once you have authenticated to the Email Attribute Tool, you will be able to view and adjust your email preferences. By default, the Email Address Lookup tool will automatically display the Preferences associated with your account.

You can view or change settings for:

- Preferred Email Address
- Email Local Addresses
- Email Forwarding Address

There are also preference settings for some anti-spam measures:

- Full Grey Listing Setting
- Discard Spam Setting

3.5.2. Your Preferred Email Address
Your Preferred Email Address is the email address publicly associated with your account. Typically, your Preferred Email Address should be set to the email address you use as the From: address when sending email, as well as the address you use when listing your address on web pages, business cards, and elsewhere.

Note: Changing your Preferred Email Address does not affect how your mail will be delivered.

Most commonly, our users opt to advertise their email address as username at cs.cmu.edu, like so:

example@cs.cmu.edu
You may also choose to advertise your email address using the full form of your name:

Edward_Xample@cs.cmu.edu

Your Preferred Email Address is published in local email directories as your primary address; if your Preferred Email Address is set to an improper or invalid address, others may be unable to send you email.

If your email is delivered locally, we recommend setting your Preferred Email Address to match one of your Email Local Addresses.

**Modifying Your Preferred Email Address**

To change the value of the Preferred Email Address attribute using the Email Attribute Tool:

1. Navigate to [https://www.fac.cs.cmu.edu/corvid/lookup/](https://www.fac.cs.cmu.edu/corvid/lookup/)
2. Click on the Modify Preferred Email Address link.
3. Type your new Preferred Email Address into the text box:

   ![Email Attribute Tool](https://www.fac.cs.cmu.edu/corvid/lookup/

4. Click **Replace Entry**.
5. Check your selection; if all is well, click **Confirm Replace Entry**.

Your request will automatically be forwarded to the Help Desk; you will be notified when the change has taken effect.

**3.5.3. Your Email Local Addresses**

Each SCS mail account is associated with a list of Email Local Addresses. These are email addresses at which the SCS email system will accept mail for delivery on your behalf.

There are several email addresses associated with your account by default.

A few of the default addresses are required for historical and practical purposes. All of the following email addresses must be associated with your account:

- username
- username+
- username+@cs.cmu.edu
Additionally, your list of Email Local Addresses may also include common combinations of first and last names at common SCS domains. For example:

- FirstName.LastName@cs.cmu.edu
- FirstName_LastName@ri.cmu.edu
- Nickname@scs.cmu.edu

**Removing an Address**

To remove one or more of the email addresses associated with your account:

1. Navigate to [https://www.fac.cs.cmu.edu/corvid/lookup/](https://www.fac.cs.cmu.edu/corvid/lookup/)
2. Click on the Modify Email Local Address link.
3. Select any email addresses you wish to remove.
4. Click **Remove Selected Entries**.
5. Check your selection; if all is well, click **Confirm Remove Entry**.

The address(es) should be removed from the list of Email Local Addresses immediately; you should no longer receive email at any of the removed addresses.

**Adding an Address**

To associate a new email address with your account:

1. Navigate to [https://www.fac.cs.cmu.edu/corvid/lookup/](https://www.fac.cs.cmu.edu/corvid/lookup/)
2. Click on the Modify Email Local Address link.
3. Type your new Email Local Address into the text box.
4. Click **Add Entry**.
5. Check your selection; if all is well, click **Confirm Add Entry**.

You request will automatically be forwarded to the Help Desk.

There are restrictions on additional Email Local Address requests:

- Do not request large numbers of additional Email Local Addresses; keep your list manageable.
- Do not request Email Local Addresses that are possibly offensive or inappropriate.
- Limit your Email Local Addresses to schools or departments with which you are associated.
- Do not include domains that are not local to our facility (as examples, the domains **gmail.com** and **andrew.cmu.edu** are not local domains).
You will be notified when the changes have taken effect.

*Note:* SCS Computing Facilities reserves the right to reject any request that is not in compliance with University Computing policies and guidelines. In addition, the requested Email Local Address may not be available. You will be notified by the SCS Help Desk if this situation arises.

### 3.5.4. Your Email Forwarding Address

All users in SCS have the ability to request where their mail is forwarded. You can specify where your mail will be delivered by setting your Email Forwarding Address. The Email Forwarding Address is a single email address where we will direct your SCS email for delivery.

Your Email Forwarding Address can be set to any one of the following:

- The SCS IMAP server (`username@imap.srv.cs.cmu.edu`)
- The SCS Exchange server (`username@exchange.cs.cmu.edu`)
- Your Andrew mail account (`username@andrew.cmu.edu`)
- An external account (for example: `username@gmail.com`)

...or any other valid email address where you accept email.

### Managing Your Email Forwarding Address

To change where your mail is delivered:

1. Navigate to [https://www.fac.cs.cmu.edu/corvid/lookup/](https://www.fac.cs.cmu.edu/corvid/lookup/)
2. Click on the Modify Email Forwarding Address link.
3. Type your new Email Forwarding Address into the textbox.
4. Click Replace Entry.
5. Check your selection; if all is well, click Confirm Replace Entry.

### Caveats

Please make sure that the delivery address you select is a valid address that accepts mail. In the particular case of external addresses, we have no way of checking if the target address is valid. If you are unsure if the target address is valid, please contact the SCS Help Desk for assistance.

If your mail is currently delivered to the IMAP server, the forwarding change will happen immediately.
If your mail is currently delivered to the Exchange server, you will need to contact the SCS Help Desk for further action. Most change requests will be resolved within one business day.

If you do choose to have your mail forwarded to an off-site account, SCS Computing Facilities will be very limited in the assistance we can provide to resolve email problems.

Please do not publish your Email Forwarding Address; your Email Forwarding Address is not meant for public use.

3.5.5. Blocking Spam With Grey Listing

Grey Listing is a mechanism for reducing spam, and works as a supplement to the existing Pure Message anti-spam service. In conjunction with Pure Message, Grey Listing has been shown to very effective for reducing the amount of spam that reaches both a user’s INBOX and SPAM folder. Grey Listing is turned on by default.

SCS Computing Facilities grey lists only email from outside the university. Email from within the university is not subject to this mechanism. By default, all new accounts have this attribute set to TRUE.

We strongly recommend against changing this setting. For more information about Grey Listing in the SCS Computing environment please refer to our Help pages at:

http://www.cs.cmu.edu/~help/mail_news/corvid/greylisting.html

Managing Grey Listing

To change the value of the Full Grey Listing attribute:

1. Navigate to https://www.fac.cs.cmu.edu/corvid/lookup/
2. Click on the Modify Grey Listing Setting link.
3. Make your selection.
4. Click Replace Entry.
5. Check your selection; if all is well, click Confirm Replace Entry.

3.5.6. Discarding Spam

As Email is received it is examined for evidence of spam (please see §1.4. Spam and Virus Detection and Filtering on page 23). If the email appears to be spam, it is tagged with the addition of the email header X-Spam-Warning.
The Discard Spam attribute will determine whether email that we believe is spam is either delivered to your Email Forwarding Address (if it is a local address) or immediately discarded.

This Discard Spam attribute can have these settings:

- **TRUE** - If it is spam, we reject or discard it as soon as possible
- **FALSE** - Deliver the email, even if it is spam

**Note:** If this setting is blank (unset), spam will be handled as if Discard Spam has been set to FALSE.

### The Effects of Offsite Forwarding on Spam Delivery

If you forward your email off-site, our servers will not, by policy, forward any mail that is flagged as spam.

Many external sites have mechanisms that limit or block hosts that send too much spam. These blocks are often temporary, but can require time to remove on the part of the receiving site.

Usually, these blocks cover all traffic from the sender's site; if an SCS user sends too much mail to example.com, the mail servers at example.com may begin refusing mail from *everyone* using the SCS servers to send mail. If the receiving site is a popular mail service like Google Mail, a block can affect many users. For this reason, we do not forward spam off-site.

### Managing Discarding Spam

To change the value of the Discard Spam attribute:

1. Navigate to [https://www.fac.cs.cmu.edu/corvid/lookup/](https://www.fac.cs.cmu.edu/corvid/lookup/)
2. Click on the Modify Discard Spam Setting link.
3. Make your selection.

- **Current Discard Spam**
- **New Discard Spam**
- **Action**

4. Click **Replace Entry**.
5. Check your selection; if all is well, click **Confirm Replace Entry**.
3.6. Mailing Lists

Mailing lists in the SCS environment are managed by the Mailman mailing list system. Some of its many features include:

- A web based interface
- Control of subscription status and delivery options
- The ability for list administrators to use their Kerberos passwords for authentication to access administrative functionality
- Moderated list posting
- Some spam control

3.6.1. Creating a Mailing List

The creation of new mailing lists is handled by the Help Desk. To request the creation of a new mailing list, please contact the Help Desk with the following information:

- The name of the mailing list.
- SCS usernames who will serve as administrators for the list (one administrator is required; at least two is recommended).

For more information about creating mailing lists, please see:
http://www.cs.cmu.edu/~help/mail_news/mailman/index.html

3.6.2. Mailing List Administration

Mailman gives list administrators the ability to do the following:

- Access administrator page for the list
- Make a list visible to the public
- Include sub lists
- Configure member posting policy
- Add members
- Assign moderators
- Configure white lists and blacklists
- Block messages that have been tagged as spam

For more information about Mailman mailing lists please see:
http://www.cs.cmu.edu/~help/mail_news/mailman/

3.6.3. Mailing List Etiquette

When sending Email to mailing lists please be considerate:

- Keep messages short
- Keep attachments small
- Avoid sending spam

If you need to send a file as an attachment that is large, please consider putting the file on a website and including a URL in your message that points to the web location of the file.
4. Printing

SCS Computing Facilities provides support for over 150 printers within SCS, along with infrastructure that allows printing from Windows, Mac, and Linux hosts.

4.1. Printing Etiquette

The public printers in the School of Computer Science are a shared resource. For that reason, members of the community should:

- Only print large jobs at night or off-hours
- Promptly pick up your printer output (and only your output)
- File output that you see
- Use the copier, not the printer, for multiple copies
- Use color printers only when necessary (color copying is more expensive than black and white)
- Use SCS printers only for SCS-related work
- Preview your output before printing

4.2. Getting Help

If you have a problem with a printer, contact the SCS Help Desk to report printing problems during normal business hours.

SCS Operations also provides 24 x 7 printer support for many printer problems, such as being out of toner, routine paper jams, etc.

SCS Operations may be reached by calling:

(412) 268-2608

More severe printer problems will need to be handled during normal business hours.

4.3. Lists of Printers

To review the full list of all available printers and their locations, please refer to:

http://www.cs.cmu.edu/~help/printing/
5. Networking

The SCS network is one of three network entities on campus. In addition to the SCS network, the other two networks are the ECE Department network managed by ECE Facilities, and the Computing Services network managed by CMU Computing Services.

The Computing Services network provides local network connectivity for everyone on campus except for users in SCS and ECE. Computing Services also provides the campus with connectivity to both the commodity Internet and research networks. The CMU Computing Services networking group manages the CMU, CMU-GUEST, and CMU-SECURE campus wireless networks.

5.1. SCS Network Use Policies

The SCS network is vital to the School's research and educational activities. We ask that you adhere to the following practices:

- Use only IP addresses that have been assigned to your host.
- Configure your machine to use DHCP.
- Use only authorized DHCP servers.
- Do not run routing software on user systems.
- Do not use unpatched or compromised hosts.
- Contact the Help Desk before performing any network-related experiments which may adversely affect network performance.
- Do not install or use unauthorized wireless access points.

To help prevent network problems and assist SCS Computing Facilities in fixing problems when they occur, people using the SCS network must abide by the network use policies given below. These policies are meant to supplement the official Carnegie Mellon computing policy and provide some SCS-specific additions to that policy.

SCS Computing Facilities reserves the right to disconnect or otherwise remove hosts and equipment from the network without notice if they:

- Cause technical issues that impede other users
- Violate network usage policies
- Use an unassigned or unauthorized network resources
- Show signs that they have been compromised

SCS Computing Facilities reserves the right to monitor network traffic in order to detect or debug network problems and to detect unauthorized use of the network or activity that violates network usage policies. We reserve the right to scan any host or equipment connected to the SCS network for open ports, possible security holes, or any other information that may be gained by scanning. By using the SCS network, or connecting hosts or equipment to the SCS network, you consent to such monitoring and scanning.
5.1.1. Connecting Hosts to the Network

You must register any host or network device that you would like to connect to the SCS network with SCS Computing Facilities. To register a device to use the SCS network, you must provide all of the following information about the device before putting it on the SCS network:

- device type
- asset tag number
- serial number
- location
- hardware address
- contact information

An exception: When registering personally owned equipment for a network connection, you do not need to provide an asset tag number.

You must notify us if any of the above information changes for any network connected device. It is especially important that SCS Computing Facilities is notified when a machine is moved. Moving a machine may require an IP address change to the machine and network connectivity may be inconsistent at best without the IP address change.

The wired network in SCS buildings belongs to the SCS network infrastructure. The wireless network is part of the campus network, and is maintained by campus Computing Services. For more about the wireless network at Carnegie Mellon, please see §1.5. Wireless Networking on page 40.

Use the Netregister form found at the following URL for all new registrations and updates of SCS network-connected devices:

http://www.cs.cmu.edu/~help/networking/netregister.html

Only in special cases will we give out an IP address without knowing the host’s hardware address.

Hosts, equipment, and cables/wiring should not be connected to the SCS network, moved to different network outlets, or reconfigured in any way that might affect network performance or functionality, without prior notification and approval of SCS Computing Facilities.

Outlets are not automatically activated. If you are moving your computer to an unused outlet, you will need to request the activation of that outlet. To request an activation make a note of the outlet number beginning with an R, which will available on a label attached to the network port and follow this form:

R00A00-000-00

Please send any activation request, including the appropriate outlet number, to help@cs.cmu.edu.
5.1.2. Host Naming Conventions
The machine naming convention here in SCS is:

\[ \text{hostname.project.department.cmu.edu} \]

- The project component of a hostname must somehow be related to SCS or CMU.
- Project subdomains will only be assigned for groups of machines relating to the project.
- SCS Computing Facilities tries to avoid having multiple hosts that have the same hostnames.
- All personally owned machines will be assigned a name in the .pc.cs.cmu.edu namespace without exception.
- SCS Computing Facilities reserves the right to reject inappropriate hostnames.

5.1.3. Network Usage Restrictions
You may not use the SCS network or data gathered from the SCS network for purposes of gaining or attempting to gain unauthorized access to hosts, networked equipment or data. Any use of the SCS network to scan, break into, attempt to break into, or intentionally degrade the performance, functionality, or network connectivity of hosts or other networked equipment is prohibited, unless:

- You have the permission of the administrator(s) of said hosts and/or equipment,
- you notify SCS Computing Facilities prior to engaging in the activity,
- and the activity will not cause service or performance problems for other hosts or equipment on the network.

Some exceptions may be granted for non-obtrusive scanning, network measurement, or other activities, but you must first notify SCS Computing Facilities as well as obtain permission before beginning any activity that could affect the network.

Network monitoring for research purposes or debugging network problems is allowed. Please contact SCS Help for assistance. Monitoring is subject to relevant federal, state or other laws. It is expected that people collecting such data will respect the privacy of anyone whose traffic is incidentally collected by such activities. Network monitoring or packet sniffing for the purposes of intercepting email, passwords, or other personal data without the consent of all parties is not permitted.

Any use of the SCS network that may possibly affect network performance, routing, connectivity, or possibly cause service or performance problems for other hosts or equipment must be approved by SCS Computing Facilities beforehand.
Using the SCS network for purposes of harassment, fraud, sending threatening communications, inappropriate sending of unsolicited bulk email, or any violation of applicable federal, state or other laws, or university policy, is prohibited.

Any use of the SCS network or hosts for commercial purposes or personal gain, except in a purely incidental manner, without advance authorization is prohibited.

5.1.4. Running Network Services
If you install, enable, or administer any network-aware software on a host, including Web, FTP, SSH, file-sharing, and operating system services, you are responsible to make sure the software does not interfere with network operation, cause problems for other hosts on the network, provide unauthorized access to hosts or data, or otherwise violate network usage policies.

You are responsible for making sure that any network-aware software that you install or administer is kept up-to-date with respect to security patches, and for taking appropriate steps to prevent unauthorized access or use of such software. Hosts or other networked equipment running software or services that are known to be insecure, or that are configured in an insecure manner, may be disconnected or otherwise removed from the network.

If a service generates a very large amount of network traffic, we will need a work-related justification and may ask you to find ways to reduce the amount of traffic.

Use of such services for illegal behavior, including illegal distribution of copyrighted materials without the consent of the copyright holder, is prohibited.

5.2. Computing Services Bandwidth Restrictions
CMU Computing Services enforces a quota of ten gigabytes (10GB) of bandwidth per day inbound or outbound over the commodity Internet connection. There is no bandwidth quota for research network traffic. For more information on CMU Computing Services usage Guidelines see:

http://www.cmu.edu/computing/network/guidelines/bandwidth.html

If you need to use more bandwidth than is allowed by campus policy, you can request an exemption from the bandwidth limit. For information about how to request a bandwidth exemption, please see:

http://www.cmu.edu/computing/network/connect/bandwidth/
5.3. Hosting Domains

If your project is using a vanity domain, we may be able host that domain. We can host domains for both website and email traffic under certain conditions.

5.3.1. Domain Hosting

- You can use equipment on the CMU 128.2.*.* IP address space to host a domain as long as it is non-profit and the domain is .org.
- SCS Computing Facilities will provide name service for a domain if the domain is related to SCS or CMU research/educational non-profit activities.
- SCS Computing Facilities does not delegate DNS for SCS or sub-domains of SCS projects.

A special address space has been set aside for non-commercial domains with a top level domain other than .org. Domains hosted in this address space must be related to the School of Computer Science and/or Carnegie Mellon University. Please contact the SCS Help Desk if you have a domain that requires this special IP address space.

5.3.2. Email for Hosted Domains

We can provide the following email services for hosted domains:

- mail aliases
- mailing lists
- mail forwarding

Email services for hosted domains are only available for domains associated with CMU sponsored research.

5.4. Remote Access

You must use your username/remote instance when using SCS Remote Access Services.

Connecting via any remote site has the potential of exposing your username and password. If someone obtains your primary SCS Kerberos username/password they could gain full access to your data. If someone obtains your username/remote instance password they will only have the ability to access the SCS remote access services (VPN and iPass). Problems could occur if either account is compromised, however, the /remote instance does not provide attackers access to your data.

Instructions on creating a /remote instance can be found at:

http://www.cs.cmu.edu/~help/accounts_passwords/create_instance.html
5.4.1. VPN
The SCS VPN (Virtual Private Networking) software allows a computer on another network to appear that it has an SCS name and IP address. Using VPN, a remote host can access restricted network services that can only be accessed by SCS hosts. The VPN client is available for Windows, Mac OS X, and Linux.

Download the VPN client for Windows, Mac and Linux systems from:
https://www.cs.cmu.edu/~help/networking/downloads.html

For a description of how to use the VPN, please see:
http://www.cs.cmu.edu/~help/networking/vpn/

5.4.2. iPass
iPass is the world’s largest virtual network including dial-up in over 150 countries and, together with the T-Mobile HotSpot network, close to 60,000 Wi-Fi hotspot and Ethernet hotel broadband locations. The iPass service provides easy-to-use, reliable access to the Internet from virtually anywhere in the world.

Download the iPass client for Windows or Mac from:
https://www.cs.cmu.edu/~help/networking/downloads.html

For a description of how to use the iPass service, please see:
http://www.cs.cmu.edu/~help/networking/ipass.html

Be sure to test the iPass service before leaving on your trip.

Check with your hotel before using iPass. Users are responsible for any local toll charges and hotel fees which may apply while using the iPass client to connect to the service.

Please do not use the iPass service from the Pittsburgh area, except to test the service. This service is intended for use while traveling and charges are billed to SCS Computing Facilities on a per minute basis.

5.5. Wireless Networking
The campus wireless network is administered and maintained by campus Computing Services.

While SCS Computing Facilities is not responsible for the campus wireless, we can help verify configuration settings. We can also work with Computing Services to report and track outages in the campus wireless networks. If you experience wireless issues please contact the SCS Help Desk.

5.5.1. Computing Services Wireless in SCS
Many users in the SCS community use the campus wireless networking service. However, there are some things to consider when using these wireless networks:
A wireless connection is not as fast or reliable as a wired connection.

You must use SCS VPN to access the following SCS services:

- Windows domain services (with some exceptions)
- Any other SCS service restricted by IP or hardware address.

Wireless is not meant to be a substitute for wired Ethernet for tasks that require large amounts of bandwidth. For example, we cannot create archival backups of hosts over the wireless network.

If you have any questions about Computing Services wireless service, contact the SCS Help Desk.

### 5.5.2. Computing Services Secure Wireless

Campus offers an encrypted wireless network that requires authentication to join. This secure wireless network is named CMU-SECURE.

You do not need to register your device to use the CMU-SECURE wireless network. To use this network, connect your device to the network named CMU-SECURE. You will be prompted for a Username and password. Use your Andrew Username and password to connect to the CMU-SECURE network. In some cases, you may be asked to verify the connection.

### 5.5.3. Computing Services Open Wireless

Campus offers an encrypted wireless network that requires registration to join. This open wireless network is named CMU.

Traffic on the CMU wireless network is unencrypted. If you have concerns about transmitting sensitive data over a clear network, we recommend either using a VPN client, or using the CMU-SECURE wireless network.

Using the CMU wireless network requires registration. To register your wireless device to work with the campus open wireless network:

1. Establish a wireless connection the wireless network named CMU
2. Open a web page with your preferred browser and follow the instructions for registering your wireless device with the CMU network, if necessary

**Note:** Register your device in the WV.CS.CMU.EDU domain in order to access SCS-specific services.

Once registration is complete, you will be directed to a web page confirming that your device now has access to the campus CMU open wireless network.

Until you have properly registered your device for use with the CMU wireless network, all network connections except to the Computing Services authorization website will fail. Please register your device before attempting to use the CMU wireless network for reaching mail servers, filesharing servers, or other types of connections.
5.5.4. Computing Services Guest Wireless

Campus offers an encrypted wireless network for temporary use by guests of the University. This secure wireless network is named CMU-GUEST. This network should not be used by current students, faculty, or staff.

This network requires an access code to join. Faculty and staff can use the Computing Services’ Event Manager to create access codes for guests to connect to the CMU-GUEST network.

For more information about the Computing Services Event Manager, please see:

6. AFS

AFS is a distributed file system providing a client and server architecture that offers:

- File sharing within a single name space
- Security
- Scalability
- Replicated read-only content distribution
- Transparent data migration

SCS Computing Facilities uses the OpenAFS client software to provide AFS service on end-user machines. The OpenAFS client software is installed and pre-configured on SCS Linux machines to allow secure and transparent filesystem access within the SCS computing environment. AFS is also used to share and store data for classes, projects, and users. Your SCS website is served from AFS. Both authentication and the appropriate authorization are required for AFS access.

6.1. Authentication

Authentication is automatic on Linux workstations when you login with your Kerberos password.

Kerberos credentials automatically expire after 24 hours and must be refreshed, even if you remain logged in. You can refresh your Kerberos credentials by using the `kinit` command from a shell window. This will prompt you for your Kerberos password.

6.1.1. Checking Authentication

Use of the `klist` command from a Linux shell window to display your current login credentials:

```
example@linux:~$ klist
Credentials cache: FILE:/tmp/krb5cc_14871_f31544
    Principal: example@CS.CMU.EDU

    Issued       Expires       Principal
    Jun 5 12:31:17 Jun 6 12:31:17 krbtgt/CS.CMU.EDU@CS.CMU.EDU
    Jun 5 12:31:17 Jun 6 12:31:17 afs@CS.CMU.EDU
```

6.2. Access Control

Permissions in AFS are granted per directory, rather than per file, and handled by Access Control Lists (ACLs) set on each directory. Variable levels of permission may be granted to users and user groups within a particular directory.

6.2.1. AFS Permissions

There are seven AFS permissions. Four permissions effect directories, and the remaining three effect file authorization.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup</td>
<td>l</td>
<td>Affords access to a directory to perform other operations, and list directory contents.</td>
</tr>
<tr>
<td>Insert</td>
<td>i</td>
<td>Allows file and directory creation or copying.</td>
</tr>
<tr>
<td>Delete</td>
<td>d</td>
<td>Allows for removal of files or subdirectories.</td>
</tr>
<tr>
<td>Administrator</td>
<td>a</td>
<td>Allows for changing of the directory ACLs.</td>
</tr>
<tr>
<td>File</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td>r</td>
<td>Allows for file reads and directory statistics.</td>
</tr>
<tr>
<td>Write</td>
<td>w</td>
<td>Allows for writing changes to files.</td>
</tr>
<tr>
<td>Lock</td>
<td>k</td>
<td>May run applications that issue system calls to lock files within the directory.</td>
</tr>
</tbody>
</table>

AFS ignores any individual file permissions except for the owner's. Read, write, and execution file modes may be removed on a file. Denying owner permissions will remove the ability for anyone to access the file, including the owner. The Access Control List is comprised of all the users and groups, and their corresponding level of authorization within a directory.

6.2.2. Displaying an Access Control List

The command line interface of a Linux shell may be used to list the membership and authorizations of a given directory with the `fs la` command:

```
example@linux:~$ fs la .
Access list for . is
Normal rights:
  system:anyuser l
  example rlidwka
example@linux:~$
```
6.2.3. Managing Access Control Lists

Owners or users with administrative permissions may edit or add additional entries to the directory’s ACL. The Linux shell command `fs sa` may be used to manage directory ACLs.

In the following session, our example user:

1. Displays the access list on their home directory using the `fs la` command
2. Sees that the user bovik has read access
3. Removes specific access rights for the user bovik using the `fs sa` command
4. Checks to make sure that access is revoked

```
example@linux:~$ fs la .
Access list for . is
Normal rights:
  system:anyuser l
  bovik r1
  example rlidwka
example@linux:~$ fs sa . bovik none
example@linux:~$ fs la .
Access list for . is
Normal rights:
  system:anyuser l
  example rlidwka
example@linux:~$
```

6.3. Managing PTS Group Memberships

Groups may contain multiple users, and allow for easy management of directories. Newly created subdirectories inherit the permissions of the parent directory, including any existing group entries. Managing similar levels of access through group memberships is easier than adding and removing individuals from many ACLs across multiple directories.

For example, you may choose to create a group as a subtext of your own username, `username:groupname`, and add that group to the appropriate directories as you would an individual user. Group creation and membership management must be done from the Linux shell with the use of PTS commands.

AFS has several special group definitions already in place. For more, please see:

http://www.cs.cmu.edu/~help/afs/afs_groups.html
### 6.3.1. Making a New PTS Group

Our example user would like to have a PTS group to manage who has read access to his home directory.

The first step is to create the group, using the `pts creategroup` command:

```
example@linux:~$ pts creategroup example:readers
Group example:readers has id -4928
example@linux:~$
```

Next, our example user must grant the appropriate access to the group with the `fs sa` command (along with the `fs la` command to make sure the Access Control List was properly modified):

```
example@linux:~$ fs sa . example:readers read
Access list for . is Normal rights:
   example:readers rl
   system:anyuser l
   example rlidwka
example@linux:~$
```

Our example user needs to add other users to the group using the `pts adduser` command:

```
example@linux:~$ pts adduser -user bovik -group example:readers
example@linux:~$
```

The command `pts membership` can be used to check who is on in PTS group:

```
example@linux:~$ pts membership example:readers
Members of example:readers (id: -4928) are:
   bovik
example@linux:~$
```

The command `pts removeuser` can be used to remove a user from a PTS group:

```
example@linux:~$ pts removeuser -user bovik -group example:readers
example@linux:~$
```

The command `pts membership` will verify the removal:

```
example@linux:~$ pts membership example:readers
Members of example:readers (id: -4928) are:
example@linux:~$
```
6.4. Updating Web Pages

Modest websites may be hosted within AFS directories. Security measures restrict the use of PHP, CGI, or other dynamic content generation; however, server-side includes which do not rely on exec may be used.

Web content should be located in an exclusive subdirectory of an AFS volume. The permissions on this directory should be configured to provide the necessary AFS access list privileges on for the website to be served by SCS web servers.

6.4.1. Setting Permissions for the Website Directory

Make a web subdirectory within the AFS volume and set the appropriate AFS ACL and permissions. The top-level directory of the volume will have different permissions than its web subdirectories.

If necessary, set the permissions on your AFS home directory so that the web servers can access your www directory:

```bash
example@linux:~$ fs sa . wwwsrv:http-ftp l
example@linux:~$
```

Then, set the permissions on your www directory so that the web servers can access your content:

```bash
example@linux:~$ fs sa www wwwsrv:http-ftp r l
example@linux:~$
```

Subdirectories created within the www directory will automatically inherit the required access list and privileges.

6.4.2. Adding Content

Content for the site may be created using any tools available on the workstation or uploaded to it. We recommend the use of SSH copy (scp) or secure FTP (sftp) for uploading your web content.

You may use any SCS Linux host where you have an account to upload content; a common choice is to use the Linux timesharing service (see §Accessing The General Purpose Linux Services on page 8):

```bash
linux.gp.cs.cmu.edu
```

If you would like to have a personal web page served by the SCS web servers, you will need to place the files that make up your website into the www directory of your AFS home directory.

6.4.3. Privacy and Access Restrictions

Websites served from AFS will honor .htaccess file restrictions. However, we do not recommend any sensitive data such as SSNs, credit card numbers, passwords, etc. to ever be stored on websites.
6.4.4. Linking Your Content to the Web Servers
If your content does not appear at the following URL:

http://www.cs.cmu.edu/~[your username]

...your content directory may need to be linked to the Web Servers. To link your content to the web servers, please contact the Help Desk.

6.5. AFS Volumes
Units of storage in AFS are referred to as volumes, and are comprised of related directories. The most common example is your home directory's volume, available via the Linux path:

/afs/cs.cmu.edu/user/username

This unified namespace is one of the advantages of AFS. You may access AFS volumes from the same path from any machine in the computing environment where AFS is installed and enabled.

6.5.1. Requesting Volumes and Quotas
Requests for academic or project volumes may be sent to help@cs.cmu.edu. Please include the following information:

- Project name consisting of 11 characters or fewer (academic volume names are pre-determined to match the SCS designated course number and year - section numbers are also available, if they are required).
- Project sponsor or course instructor, and one additional individual to be granted full administrative rights within the volume.
- The initial quota request; please limit it to meet your current requirements (it may be resized to meet your future requirements as they change).

Classes may request drop box student directories; please include a class roster of only the student usernames, and designate TA usernames to be added for administration of volume contents when requesting a drop box.

There are different classifications of volumes that may be found within the cs.cmu.edu cell hierarchy. The following summary provides a brief description of the types, their locations, and quota assignments.
### Introduction to SCS Computing

<table>
<thead>
<tr>
<th>Volume Type</th>
<th>Description</th>
<th>Default Quota</th>
<th>Max Quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Home directory. Moderate data requirements. /afs/cs.cmu.edu/user/username</td>
<td>1 GB</td>
<td>10 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Academic</td>
<td>Class directories for sharing common documents. Student dropoff directories available upon request. /afs/cs.cmu.edu/academic/class/classno-termYear</td>
<td>1 GB</td>
<td>25 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project</td>
<td>SCS Affiliated projects may request space for collaboration purposes. /afs/cs.cmu.edu/project/projectname</td>
<td>1 GB</td>
<td>25 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup</td>
<td>Backups for existing volumes made nightly. /afs/cs.cmu.edu/.BACKUP/path-to-main-volume</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restored</td>
<td>Volumes requested for restore. Making requests as soon as possible increase the likelihood of a specific date being available. /afs/cs.cmu.edu/.RESTORED/path-to-main-volume</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Each volume has a flexible quota assigned to it. The quota may shift in size with the requirements of the volume without adversely affecting the content or availability of the volume.

Quota usage may be determined through the command line interface in a Linux shell using the `fs lq` command:

```
example@linux:~$ fs lq
Volume Name                   Quota       Used %Used   Partition
user.example                 1000000         25    0%          0%
example@linux:~$
```

If you require additional quota, please contact the Help Desk.

### 6.6. Backups and Restores

All AFS volumes receive nightly, incremental backups unless specified otherwise. User volume backups from the previous day may be accessed through the symbolic link `OldFiles` in home directories or within the corresponding backup hierarchy.

<table>
<thead>
<tr>
<th>AFS Location</th>
<th>Backup Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>/afs/cs.cmu.edu/user/username</td>
<td>/afs/cs.cmu.edu/.BACKUP/user/username</td>
</tr>
<tr>
<td>/afs/cs.cmu.edu/project/projectname</td>
<td>/afs/cs.cmu.edu/.BACKUP/project/projectname</td>
</tr>
<tr>
<td>/afs/cs.cmu.edu/academic/class/classnum-termYear</td>
<td>/afs/cs.cmu.edu/.BACKUP/academic/class/classnum-termYear</td>
</tr>
</tbody>
</table>

Volume restores for specific days are more readily available for dates within a week of the requested date, otherwise the nearest incremental backup will be used. Please make restore requests as soon as possible.
7. End-User Computing

SCS Computing Facilities can provide support for CMU owned end-user equipment. All CMU provided equipment is under full hardware and software support by default.

7.1. General Support

7.1.1. Hardware Support

What We Cover

Hosts covered by hardware support are entitled to the following:

- Warranty processing and component replacement of failed hardware, troubleshooting, & diagnostics
- Out-of-warranty component replacement of failed hardware (cost of hardware not covered)
- Uninterruptible Power Supply (UPS) for use if there is ever a power-loss event

We can service laptop batteries on supported machines after diagnostic testing has identified that the battery needs to be replaced. Battery replacement due to normal wear and tear is not covered, but should a battery experience an early failure, its replacement will be covered if the machine is under warranty.

Moving Equipment

If you need to move supported hardware, we are happy to assist. Contact the Help Desk to schedule a technician to move your equipment to a new location.

You may choose to move your equipment yourself. If you are moving equipment that connects to the wired network, you may need to request an outlet activation at the new location; please see Connecting Hosts to the Network on page 35. Please make sure to notify us of any equipment you have moved; list the old location, the new location, and the asset number of the equipment in an email to help@cs.cmu.edu.

Unsupported Equipment

We do not support personally owned equipment. You should contact your computer manufacturer directly for all problems, diagnostics, and repairs of personally owned computer equipment.

We can help with connecting personally owned equipment with the SCS Computing Environment. For personally-owned equipment, we support connecting to printing, wireless, and other computing services on a best-effort basis.
7.1.2. Backups

The data that you create is the lifeblood of your work, therefore it is critical that it is protected from accidental loss either caused by system failure, inadvertent deletion, viruses, or theft of your device. Since different users have different data protection needs, CMU/SCS Computing Facilities provides several different data protection methods:

**Standard Data Protection**

Recommended for mobile and most desktop systems. This system features real-time backup of your data, multiple restore points for data that has changed, and immediate restore of data to any device.

**Archival Data Protection**

Recommended for servers and some desktop systems. This system features nightly backups of your system, archival to tape for long-term, offsite storage, and operator-assisted restores of your data.

**Email Data Protection**

All CMU/SCS Computing Facilities supported email servers are automatically backed up every night to a tape archival data protection system.

**AFS File Servers**

All CMU/SCS Computing Facilities supported AFS servers are backed up every night to a tape archival data protection system.

Why would you pick one data protection method over another? These examples might help:

- If you have a laptop that is frequently not on the SCS Wired Network, you should choose Standard Data Protection.
- If you have a desktop that is used for normal office functions (word processing, email, etc.), you should probably choose Standard Data Protection.
- If you have a desktop that is used for research, or that has SCS business critical data, you should choose Archival Data Protection.
- If you have a server machine, especially one in one of the SCS machine rooms, you should choose Archival Data Protection.

If you have questions about which service to choose, please contact SCS Computing Facilities.

In order to receive backups, a host must be running an SCS Computing recognized operating system. There is a monthly charge for machine backups.
Important note: Hosts are not subscribed to either the Standard or Archival Data Protection systems by default. These services must be specifically requested.

**Backup Status Dashboard**

You can check the status of user data protection for all of your subscribed machines using the Backup Status Dashboard (SCS login required). Additional information about using this tool is available here:

http://www.cs.cmu.edu/~help/backups_restores/

**Restrictions on Backups**

- We may not be able to provide backups for hosts with unusual software or hardware configurations, extremely large disks, or that have large amounts of data that change on a daily basis.
- If your system is connected via wireless, dial-up, or DSL connection, only the Standard Data Protection system is supported.
- We do not back up databases, virtual OS images, or specific directories/files.
- On all platforms, the backup system is not able to back up open files. Therefore, it is important to close long-running programs (e-mail, calendar programs, etc.) before backups run in order to make sure that data files get backed up successfully.

**Dual-Boot Hosts**

We can provide backups for dual-boot hosts, but backups must be requested for each operating system for which backups are desired. Only the operating system that is running at the time backups are scheduled will be backed up. If you have a file that you know that you would like to be backed up, please make sure that you leave the machine booted overnight into the operating system that the file resides on in order to increase the chances that it get backed up.

**7.1.3. Restores**

In order to request a file restore, you must send the following information to the SCS Help Desk at help@cs.cmu.edu:

- The name of the workstation or personal computer.
- The name of the disk area, partition, and/or volume involved.
- The cause of the file loss (accidental removal, disk failure, etc.).
- The current status of the affected disk area, partition, or volume.
- The date at which you believe the file/volume/partition to have been damaged, or from which you would like to restore.
- The complete file names of the lost files.
- The time files were last modified (or created).
- The time files were lost or destroyed.
Insufficient information may delay the restore process.
Before requesting a restore on an AFS volume please check the 
OldFiles directory in your AFS space:

/afs/cs.cmu.edu/user/username/OldFiles

If the OldFiles directory is not available, please contact the Help Desk 
for further assistance.

7.1.4. VM Support
We offer support for a wide range of virtual hosting solutions across 
all supported platforms. Virtual hosting is available for machines that 
are subscribed to software support.

VMs are not backed up unless backups have been enabled for that 
VM. The backup client must be installed on the VM host and an 
additional backup support fee will apply. VMs must have a dedicated 
IP address, and run on machines with a wired ethernet connection to 
be eligible for backups.

Windows-Hosted VM Support
VMware Player is a supported package for desktop virtualization of a 
hosted OS on a Windows PC.

Linux-Hosted VM Support
On SCS Ubuntu Linux machines, VirtualBox is a supported package, 
available through standard package support tools.

Mac-Hosted VM Support
We support Parallels for desktop virtualization if you would like to 
run a hosted OS on your Mac.

Users are responsible for purchasing the Parallels virtualization 
software. If requested, SCS Computing Facilities will provide 
Windows for the VM for machines subscribed to software support.

7.2. Microsoft Windows Support
SCS Computing Facilities support for Windows-based hosts includes 
hardware support, installation and support of a baseline software 
environment, and network backups (if explicitly requested) for SCS 
owned machines. Additionally, SCS Computing Facilities technicians 
are trained and certified to provide service and perform on-site 
repairs on Dell and Lenovo machines, both in and out of warranty.

SCS Computing Facilities supports most modern versions and 
configurations of the Microsoft Windows operating system. For more 
information about Windows support, please see:

http://www.cs.cmu.edu/~help/windows/
7.2.1. Software Support
Windows machines built by SCS Computing Facilities are configured with preinstalled software. The baseline software collection is available for distribution from the SCS Windows software distribution host.

For more information about obtaining windows software, please see:

http://www.cs.cmu.edu/~help/windows/get_windows_software.html

Additional software is available from SCS and CMU Windows software distribution servers.

7.2.2. Recommended Hardware
Our recommended hardware configurations for new computer purchases can be found at:

http://www.cs.cmu.edu/~help/purchasing/recommended_pcs.html

To purchase through SCS Computing Facilities, please use the purchase request form:

https://webapps.cs.cmu.edu/PurchaseRequest

7.2.3. Printing
Detailed instructions for printer setup under Windows can be found in our SCS Help Pages:

http://www.cs.cmu.edu/~help/printing/

7.2.4. Backups and Restores
Backups of Windows hosts are not enabled by default. You must specifically request that SCS Computing Facilities back up your computer. Backups incur an additional monthly charge. If you would like to enable backups, please contact the SCS Help Desk.

7.3. Ubuntu Linux Support
SCS Computing Facilities software support for Linux hosts involves installing an SCS specific Linux environment that provides the means for remote administration, software distribution, network backups, and other services.

Support for Ubuntu Linux PCs includes: network backups (if explicitly requested), and hardware and software support. Users incur a monthly charge for this support.

Software support is unavailable for laptops running Linux.
7.3.1. **Software Support**

The SCS Computing Facilities supported Linux environment is based on the most recent Long Term Support release of the Ubuntu operating system. In general, all Ubuntu packages found in a standard install are present.

The system command `apt-get` can be used to install any needed software that is not currently installed on your computer.

We offer some popular software as packages that are tailored for use with the SCS environment:

- Mathematica
- Matlab

These packages are available for installation via the `apt-get` package management tool.

Home directories are located on local disk by default. Local home directories should be placed in `/usr0/home` or some other partition which is backed up on a regular basis.

Home directories can also be placed in AFS by request.

If the computer is under backup support, only `/etc` and directories of the form `/usrN` are usually backed up. Directories in other places, such as `/var/mysql`, are not backed up by default.

7.3.2. **Recommended Hardware**

Our recommended hardware configurations for new computer purchases can be found at:

http://www.cs.cmu.edu/~help/purchasing/recommended_pcs.html

To purchase, please use the purchase request form:

https://webapps.cs.cmu.edu/PurchaseRequest

7.3.3. **Printing**

Detailed instructions for printer setup under Linux can be found in our SCS Help Pages:

http://www.cs.cmu.edu/~help/printing/

7.3.4. **Backups and Restores**

Backups are available upon request. To have backups added to your machine, please send your request to help@cs.cmu.edu asking for backups to be added and include the name of your machine.
7.4. Apple Mac Support

SCS Computing Facilities is an authorized Self-Service Provider for Apple, Inc. Our trained technicians are Apple certified and are able to perform on-site service repairs for all Apple computer hardware, both in and out of warranty.

Support for Mac computers includes installation of a baseline software environment, network backups (if explicitly requested), and hardware and software support. Users incur a monthly charge for this support.

7.4.1. Centralized and Self-Service Support

As part of the Mac environment, SCS Computing Facilities offers enrollment in a service that allows us to centrally support Mac computers in the SCS Environment. This service is supported by the Casper Suite software from JAMF.

Casper Suite is a centralized maintenance system that makes it simpler to manage software, install printers, and easily perform troubleshooting steps. SCS Mac users can perform these tasks themselves, or rely on SCS Computing Facilities Staff to maintain their machines remotely. Casper Suite also makes it easy to run repair and diagnostic tools for both the user and administrators.

For more information about how Casper Suite can be used in the SCS environment, please see:

http://www.cs.cmu.edu/~help/macintosh/jamf/

7.4.2. Software Support

Mac computers built by SCS Computing Facilities are shipped with preinstalled software. The baseline software collection and additional software packages are available through the Self Service application.

For more information about obtaining Mac software, please see:

http://www.cs.cmu.edu/~help/macintosh/jamf/

7.4.3. Recommended Hardware

Our recommended Apple product hardware configurations can be found at:

http://www.cs.cmu.edu/~help/purchasing/recommended_pcs.html

To purchase, please use the purchase request form:

https://webapps.cs.cmu.edu/PurchaseRequest
7.4.4. Printing
SCS Mac computers use the Self Service application to manage printers. The Self Service application is installed as part of the Casper Suite of management software. For more information about Self Service and the Casper Suite, please see §7.4.1. Centralized and Self-Service Support on page 57.

Detailed instructions for printer setup for Mac OS X with Self Service can be found in our SCS Help Pages:

http://www.cs.cmu.edu/~help/macintosh/jamf/index.html#printing

7.4.5. Backups and Restores
See the Mac backup documentation for details on our Mac backup system and the limitations on what we can back up. Note that Macs will not be put into the backup system (and thus will not receive backups) unless specifically requested.

http://www.cs.cmu.edu/~help/backups_restores/mac_backups.html
8. Network & Email Security

8.1. Network Security

8.1.1. SCS Network
There is no firewall between the SCS network and the Internet. Hosts on our network are constantly being scanned for security vulnerabilities by would-be intruders, and there are numerous break-ins to SCS hosts each year. Almost all of these break-ins are preventable, and most are due to either weak passwords (often cracked via brute-force SSH attacks) or poorly configured or unpatched web applications (Wikis, phpMyAdmin, etc).

8.1.2. To Protect Yourself and Your Computers
- Always use strong passwords, including for temporary accounts and accounts you’ve created in the process of installing a software package. This can’t be emphasized enough.
- Securely configure software you install. This includes using strong passwords for services exposed to the network and restricting access to sensitive services, such as a web application’s administrative console. If you are installing a network-aware software package, you should never trust its default configuration to be secure.
- Keep software you install, particularly software exposed to the network, up to date with patches. If you do not keep your software up to date, there is a good chance that the host running the software on will eventually be compromised.
- Do not send sensitive data, such as passwords, unencrypted over the network.

If you think your machine has been broken into, contact the SCS Help Desk as soon as possible. Even if your machine is not supported by SCS Computing Facilities, you should still let us know about the intrusion.

8.2. Phishing

8.2.1. What is Phishing?
Phishing is a type of email scam that involves a fake email purporting to be from a bank, Paypal, or some other reputable source that asks you to visit a particular website (usually via a link that is included in the email) and enter personal information. The email is really from a scammer, and the website listed in the mail is run by the scammer for
identity theft or other purposes. In many ways, protecting yourself from such internet scams is no different than protecting yourself from scams that do not involve the internet.

8.2.2. Things to Remember

Keep in mind that:

- Phishing emails are often urgent in nature and will include some reference to the need for personal, confidential information as quickly as possible.
- It is easy to forge email such that it appears to be from a company or educational institution and contains logos and other “evidence” that it is legitimate.
- It can be very difficult to tell where a link on a web page actually goes without very careful inspection. So, you do not know if clicking on such a link will take you to the company’s real website.
- If you suspect that the email may really be from your bank or other institution, call their customer service number (which you have gotten from known legitimate documents) to confirm its authenticity. If the email purports to be from SCS Computing Facilities, contact the SCS Help Desk at (x8-4231).
- Never send your SCS or Andrew login information (or any other confidential information) in response to an email. We will never ask you to do so.

8.2.3. What to Do

In the case that you receive an email and suspect that it is a phishing attempt, do not open any attachments or click on any links associated with the email. Delete any such email immediately.

- Immediately change any password(s) you may have typed at the site. If you typed your Andrew password at the site, contact the CMU Information Security Office (iso-ir@andrew.cmu.edu).
- If any of the passwords you typed are the same as, or similar to, other passwords you have, those passwords must be changed, too. This includes other SCS passwords, and passwords for other sites. such as your Andrew account, and accounts for banking, social media, etc.
- Because your main SCS Kerberos password allows you to change your SCS Windows Domain password, your /mail instance password, and your /remote instance password, after you have changed your main Kerberos password you should change those passwords as well.
- Scan your PC with an up-to-date anti-virus program. The site you visited may have contained malware targeting your browser or browser plug-ins, such as Flash.
CMU Computing Services has a site that checks your browser for un-patched plug-ins:
https://www.cmu.edu/iso/patch-check/

- You may wish to review Computing Services documentation on how to avoid phishing attacks, and take the on-line training courses mentioned at the bottom of that page:
https://www.cmu.edu/iso/aware/be-aware/phishing.html
9. Conclusion

Thank you for reading the Introduction to SCS Computing.

While we hope that this document has provided a gentle and comprehensive introduction to computing at the School of Computer Science, we also know that we have a large and complicated computing environment.

If you have any questions about anything contained in this document, please let us know; we would like to make sure that all of the material presented here is complete and easy to understand.

If you discover that there is material that is not adequately covered by this document, please tell us; while we can’t cover everything in complete detail, we are always eager to learn where and how we can improve the material presented in this Introduction.

As you explore the SCS computing environment, we are more than happy to offer explanations, field requests, and provide whatever assistance we can to make your work your focus.

Thanks!