Spam: in our email system

What is spam?

Spam is swamping your email or Newsgroup with many copies of the same unwanted, unsolicited e-mails, to force propositions onto people. Most spam is commercial advertising, sale of prescription drugs or doubtful products, get-rich-quick schemes, defraud attempts, extreme pornography or similar. In most cases, spam will appear merely as unwanted junk e-mail advertising but there is a substantial amount of spam now that includes computer viruses and worms.

Remember; UWS IT WILL NOT email you, to ask you;
- For your login and/or password.
  Never ever give someone your password. This is a breach of the Acceptable Use Policy and means that that person or others have the opportunity to use your account and make it appear to be you. No one wants to be blamed for the actions of another.
- To confirm or change your details.
  IT does not need this information they already have it.
- To run a Fix or Patch.
  The file probably contains a virus. UWS Applications are delivered without the user having to run anything.
- Ask for your Credit Card Details.
  IT do not need your details. If the message appears to come from a bank it is junk email. Again, Banks do not need this information they already have it. This type of email will collect your information and use it to purchase things or do other damage using your name.

How to identify Spam

Spam email can generally be identified by their Sender, Subject or Content.
On Spam, the sender's name that appears is generally a fake email address so you cannot reply to this email but the real sender can tell if you opened the email and this may lead to a proliferation of more junk mail.
If the Subject includes something that is distasteful or you don’t understand like; Re[] it probably is Spam. Be aware also of no Subject as well. This may be harmless because some people just forget to put a Subject on it.
The content of course says it all.

Reading Pane

In outlook you should always use the Reading Pane to view you emails. So if you aren’t sure about the Sender or Subject, then selecting the email will make the content appear in the reading pane.
Note the Reading Pane DOES NOT OPEN the email (regardless of the I con symbol) but you can read the contents and even open attachments or links from it, if you are sure it’s not junk email.
How do they get my address?
Spammers get email addresses from lists which are not securely kept. Mass mailing virus's regularly scour an infected machine for email addresses and then randomly fill out the To and From fields with you details. Normally the only address they leave out is the address associated with infected machine. Spammers can also use programs to lift email addresses off the web pages. They will also use links on these pages to go to other pages and collect addresses.

There is a group called Hosted Scripts who invite people to use their page as a link from your page, they even give you the HTML script. The site is; http://members.hostedscripts.com/antispm.html
The following is lifted straight from their Anti Spam page.
“This page has one hundred randomly generated email addresses (reload and new ones will appear). At the bottom of the page is a link to this page again, essentially reloading it for programs to collect more fake email addresses. Email collecting programs will be sent in an infinite loop by following the link at the bottom of the page and will get more and more fake email addresses stuck in their databases. This helps to place many invalid email addresses that won’t help spammers (they will get more returned email ;) and is our effort to fight spam.”

What is the UWS doing about Spam?
Currently IT captures about 40% of the Spam that you won’t see and identifies more emails that may be spam and identifies them for the user. (You may see the word “Spam:” in the Subject)
With current software upgrades IT expects to identify and delete even more.
The problem IT faces is that it can’t be absolutely sure it is Spam or a message for the user.
Later this year IT will introduce 2 measures that will help in the fight against Spam
 IT will introduce a enterprise wide Personal firewall on most Windows desktop computers. This will allow IT to centrally control the settings while allowing some users to change their settings for their particular users needs.
 IT will be moving to an Anti Virus product from Computer Associates as it allows for Virus Signatures to be deployed more quickly, logs from Anti-virus software will be collected centrally and reports will be generated on how up to date workstations are with their Antivirus software.

fact: did you know that during a recent Email virus outbreak, the Anti-virus email gateways removed 70,000 emails in an hour that were infected with virus's. This doesn't include thousands more that had their infective material replaced with a txt message on the exchange server.
What to do with Spam? (or more importantly what not to do with it)

Here are the main tips for Spam emails;
- Do not open the email.
- Use the Reading Pane to view contents.
- Do not open or run any attachments unless you requested them. Even if they appear to be from someone you know. A virus is unlikely to be sent from the person that the email says its from and if you haven’t asked for an attachment, particularly and executable attachment, then there is a good chance that it didn’t come from the person.
- Do not join a group or newsletter list or the equivalent unless you are sure it is safe to do so
- Do not give your email address away unless you are sure of their security.
- Delete spam emails completely from of Outlook. Using Shift + Delete will delete the message completely, bypassing the Deleted Items folder.
- Create a “Rule” to identify keywords and send them to the Junk Mail Folder. Check this folder periodically, with the Reading Pane, and delete the Spam from Outlook. This way you don’t have to do it so often.

What to do if you think your machine may be infected?

If you think you have a virus, the first step is to contact the ITD helpdesk on Ext 5111 and they will guide you through a series of questions and assist you to determine whether further action is needed. They will also log a call for User Support Officers or IT Security to assist you with reassuring whether further investigation is needed.

On another note,
Spare a thought for the Hormel food company who produce a canned meat product. They are probably still wondering how they happened to be chosen as the icon of so much bad will on the internet.